

UNITED STATES DISTRICT COURT
Western DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF)
THE PREMISES LOCATED AT: 604) No. 23-SW-03006-WJE
Upland Creek Road Columbia, Missouri)
65201 located in the Western District of) **FILED UNDER SEAL**
Missouri.

SIGNED AND SUBMITTED TO THE COURT FOR
FILING BY RELIABLE ELECTRONIC MEANS

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Thomas Putting, a Special Agent with Homeland Security Investigations, being first
duly sworn, hereby depose and state as follows:

INTRODUCTION AND BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 604 Upland Creek Road Columbia, Missouri 65201 which is located in the Western District of Missouri (hereinafter the “SUBJECT PREMISES”), further described in Attachment A, for the things described in Attachment B.

2. I have been employed as a Special Agent (“SA”) of the U.S. Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (“HSI”), since March 2019, and am currently assigned to the HSI office in Saint Louis, Missouri. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center (FLETC) in Brunswick, Georgia, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the

opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252(a), and I am authorized by law to request a search warrant.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (production of child pornography), 18 U.S.C. § 2252A(a)(1) and (2) (distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography) (hereinafter the “SUBJECT OFFENSES”) are presently located at the location to be searched, and within computer(s) and related peripherals, computer hardware and media, and wireless telephones found at that location.

LOCATION TO BE SEARCHED

5. The location to be searched (the “SUBJECT PREMISES”) is located at 604 Upland Creek Road Columbia, Missouri 65201, is a single-story residence with tan brick and a brown roof. The front door of the residence is blue and “604” is on the left side of the garage and painted on the curb next to the mailbox. A photograph of the home is attached to this Affidavit and labeled as “Attachment A”.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:
- a. “Cache” refers to text, image and graphic files sent to and temporarily stored by a user’s computer from a web site accessed by the user in order to allow the user speedier access to and interaction with that web site.
 - b. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.
 - c. “Child pornography,” as defined in 18 U.S.C. § 2256(8), includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, or the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
 - d. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones and wireless telephones.
 - e. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit

electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

- f. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- g. “Geo-located,” as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.
- h. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
- i. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.
- j. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections

between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

- k. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
- l. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, sharing photos or videos, reading a book, or playing a game.
- m. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.
- n. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.
- o. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.
- p. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion

into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

- q. The term “web site” consists of text pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol.
- r. “Wireless telephone or mobile telephone, or cellular telephone or cell phone or smartphone” as used herein means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

COMPUTERS AND CHILD PORNOGRAPHY

7. From my own training and experience in the area of Internet-based child exploitation investigations, and through consultation with other knowledgeable law enforcement officials, I know the following to be true. Computers connected to the Internet identify each other by an Internet Protocol (“IP”) address. An IP address can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead a law enforcement officer to a particular Internet service company and that company can typically identify the account that uses or used the address to access the Internet.

8. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. To distribute these images on any scale also required significant resources. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and wireless telephones, child pornography is traded through the Internet, by using, for example, file sharing software.

9. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera, as well as from a wireless telephone. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

10. The Internet allows any computer (including wireless telephone) to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs which allow subscribers to connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

11. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) Web sites that offer images of child pornography. Child pornography collectors can use standard Internet connections to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache to look for "footprints" of the Web sites and images accessed by the recipient.

DESCRIPTION OF CASH APP

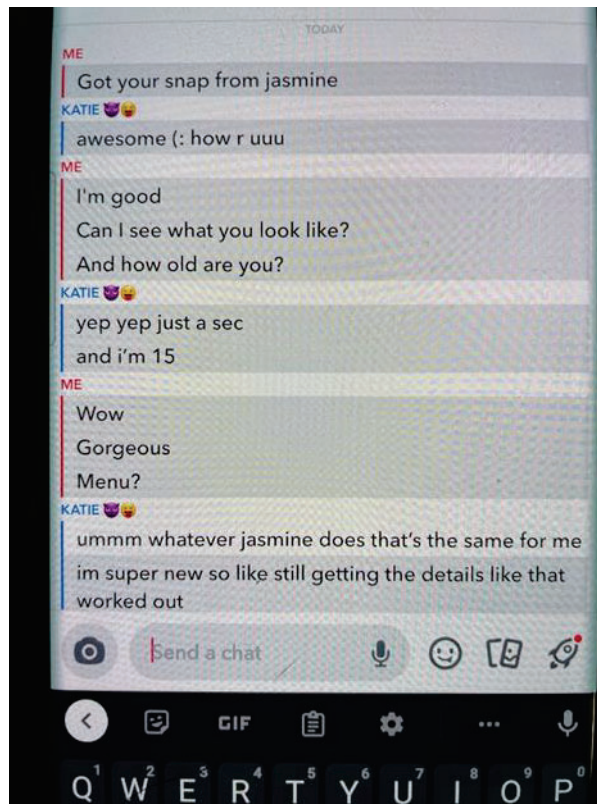
12. The Cash App is a mobile payment service available in the United States and the United Kingdom that allow users to send or receive money to one another using a mobile phone or desktop application.
13. Users create an account using their phone number and/or an email address. Cash App then sends a secret code via text or email to verify the account. Users then create a “\$Cashtag”, which is a unique username to the user. This “\$Cashtag” can be used for Cash App users to find one another to send or receive money. This “\$Cashtag” can be changed at anytime in the users account settings.
14. Users can request a “Cash Card” Visa Debit card that is connected to the Cash App account at any time.

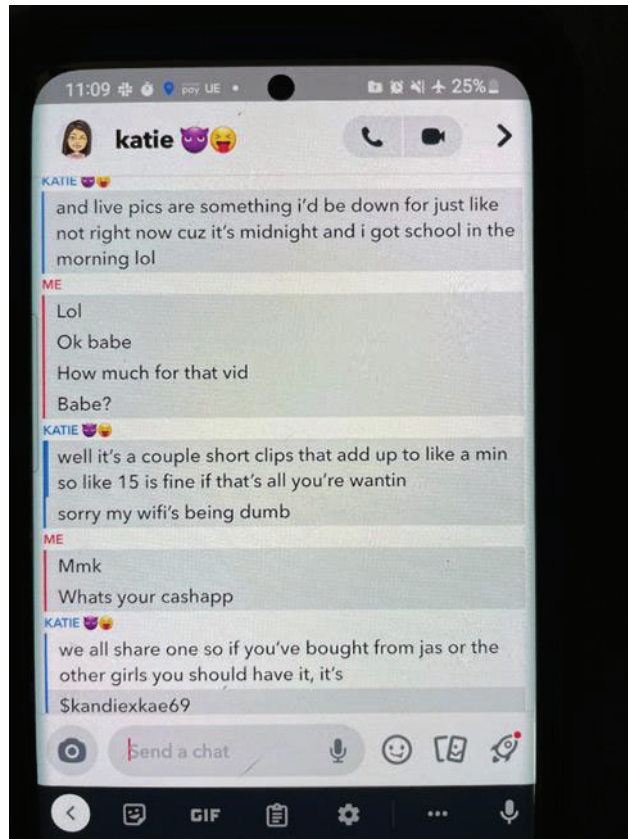
PROBABLE CAUSE

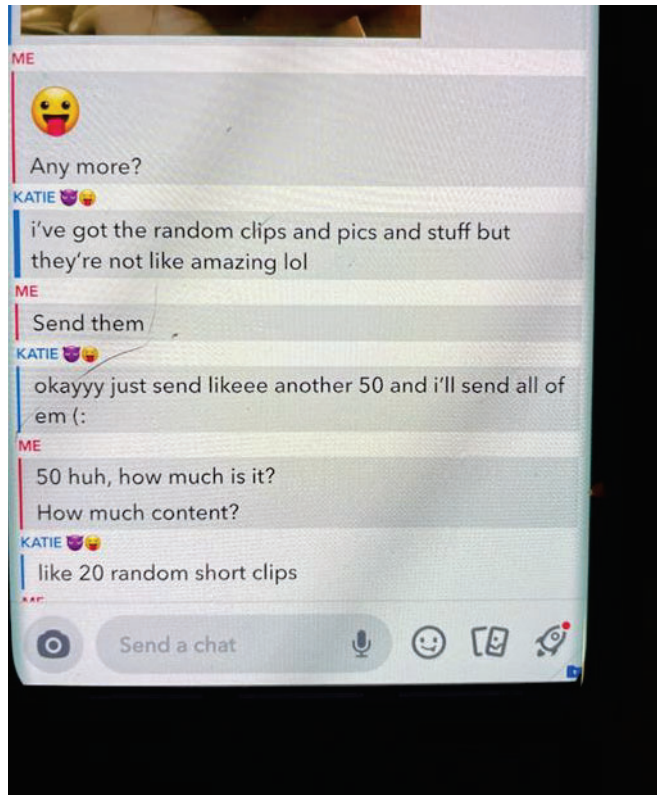
15. On or about March 29, 2022, Nabeen Leigh Singha (henceforth known as SUBJECT BUYER) arrived at Newark Liberty International Airport aboard a flight from the Toronto, Canada. Upon his return to the United States and arrival at the airport, law enforcement conducted a border search of the luggage in SUBJECT BUYER’s possession. Law enforcement located a black Samsung Galaxy S21 Ultra 5G cellphone (“SUBJECT BUYER Phone”), with International Mobile Equipment Identity Number 353388681478246, in the possession of SUBJECT BUYER at the time of the border search.
16. Law enforcement conducted a preliminary search of the SUBJECT BUYER Phone pursuant to border search authority. Upon conducting a preliminary search of the

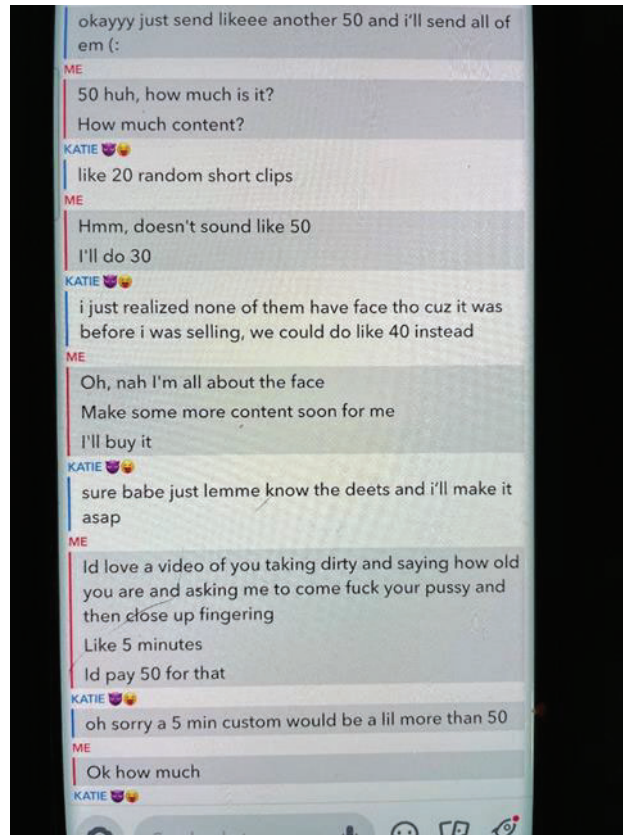
SUBJECT BUYER Phone, law enforcement identified multiple exchanges of sexually explicit messages via Snapchat application between SUBJECT BUYER and female Snapchat users, including an individual user, who goes by the name “Katie”, who identified herself as a fifteen-year-old, minor female (henceforth known as MFV-1). The conversation was explicit as to customized sexual acts that MFV-1 would film and produce for purchase at the request of SUBJECT BUYER. SUBJECT BUYER and MFV-1 discussed payment amounts and particular payment platforms. Law enforcement has since identified MFV-1 as a 14-year-old female who was 13 years old at the time the images from the conversation were produced.

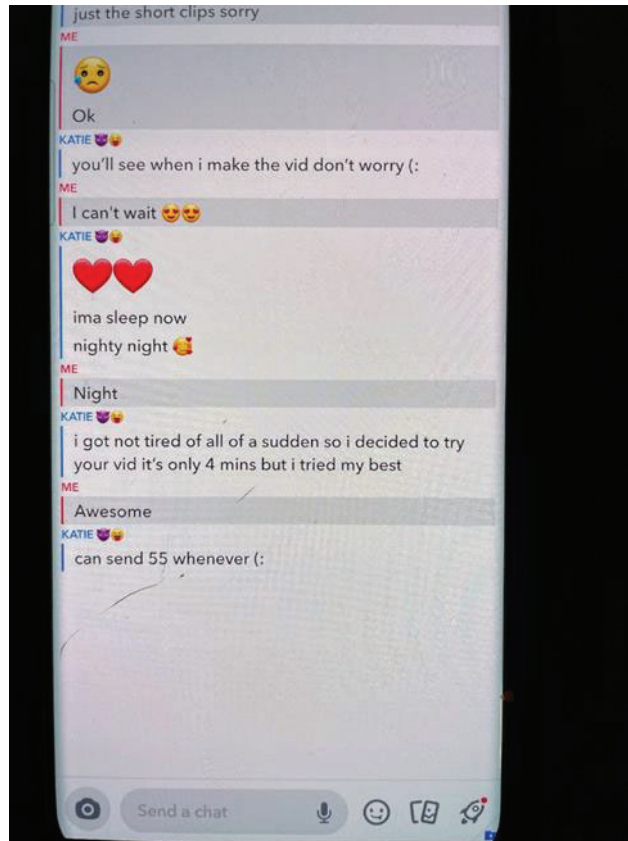
17. Law enforcement photographed the following exchanges between SUBJECT BUYER and MFV-1 within the Snapchat application of the SUBJECT BUYER Phone:









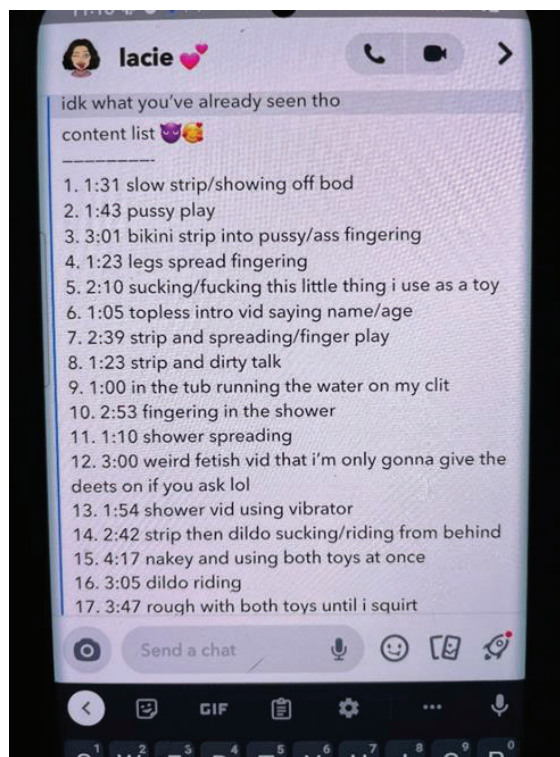


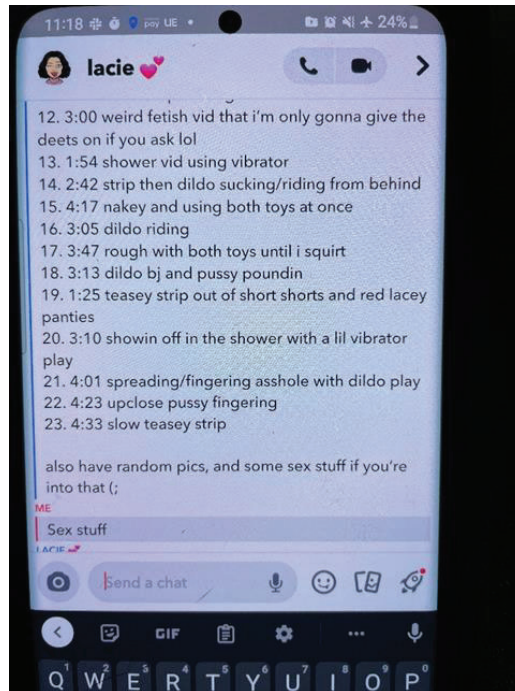
18. Additionally, a lawful search by law enforcement of the SUBJECT BUYER's phone, along with records provided by Cash App, revealed that multiple payments from a Cash App account controlled by SUBJECT BUYER, "Jason X - \$jasonvorhees666" were made to the Cash App "Kandie Kae - \$kandiexkae69". The Cash App "Kandie Kae - \$kandiexkae69" was the same account referenced in the above Snapchat conversations between SUBJECT BUYER and MFV-1, discussing payment for child pornographic videos and images.
19. In or about October 2022, law enforcement interviewed MFV-1 and MFV-1 stated they were not in control of the Snapchat account "katiexkae69" in March 2022 when this conversation took place. MFV-1 identified Ryan HINE as the creator and controller of the "katiexkae69" Snapchat account at that time. MVF-1 stated that HINE, while utilizing

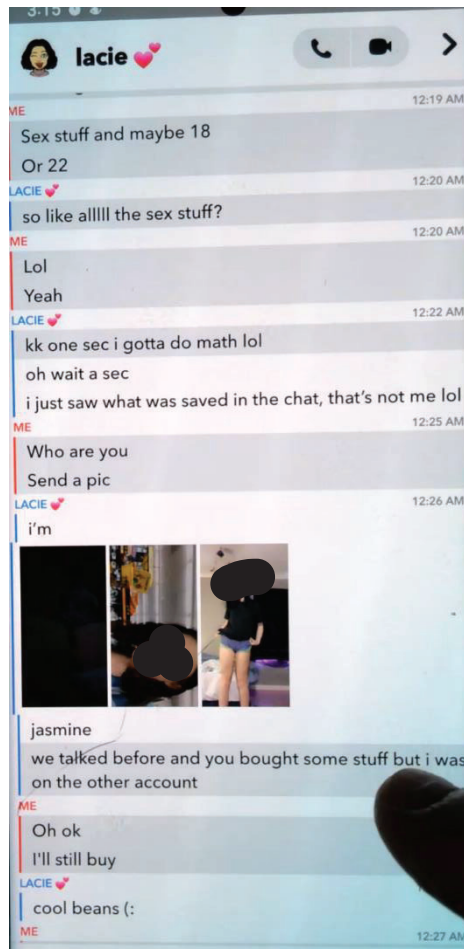
the “Kandie Kae - \$Kandiexkae69” Cash App account, paid MFV-1 for producing CSAM that was distributed to SUBJECT BUYER after his purchase in March 2022.

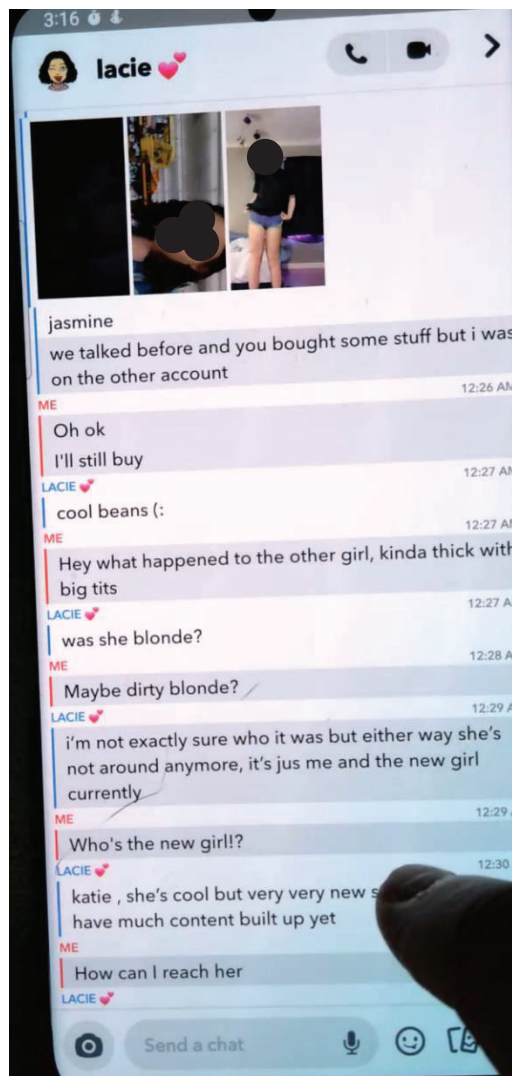
20. On or about April 29, 2022, a search warrant for the SUBJECT BUYER Phone was issued by the court (*See 22-11152 issued by the Honorable Andre M. Espinosa on April 29, 2022*). A lawful search and forensic extraction of the SUBJECT BUYER Phone was completed.

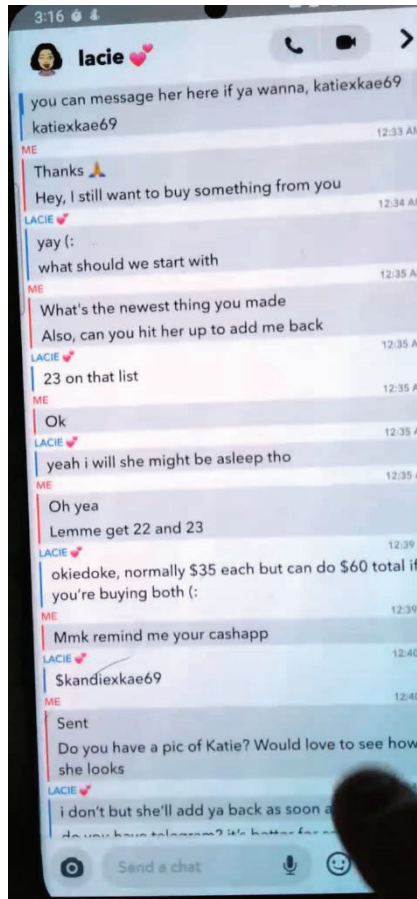
21. Law enforcement photographed the following exchanges between SUBJECT BUYER and “Laciexlove69 - Lacie” within the Snapchat application on the SUBJECT BUYER Phone:

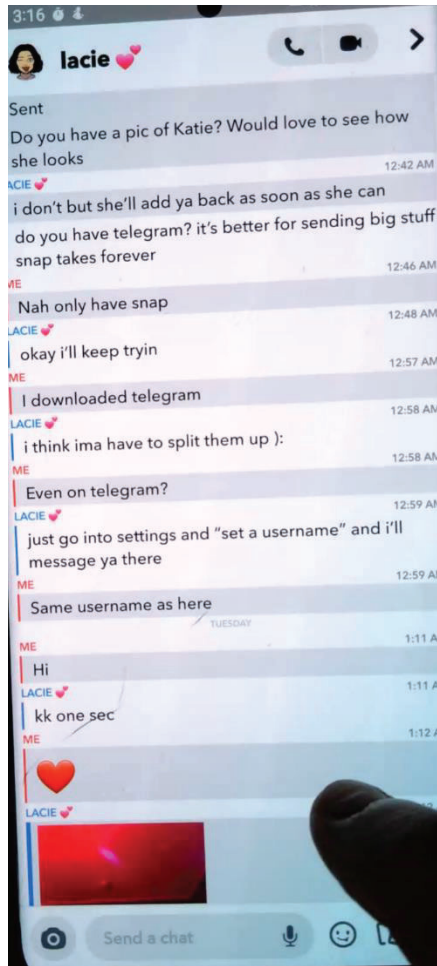








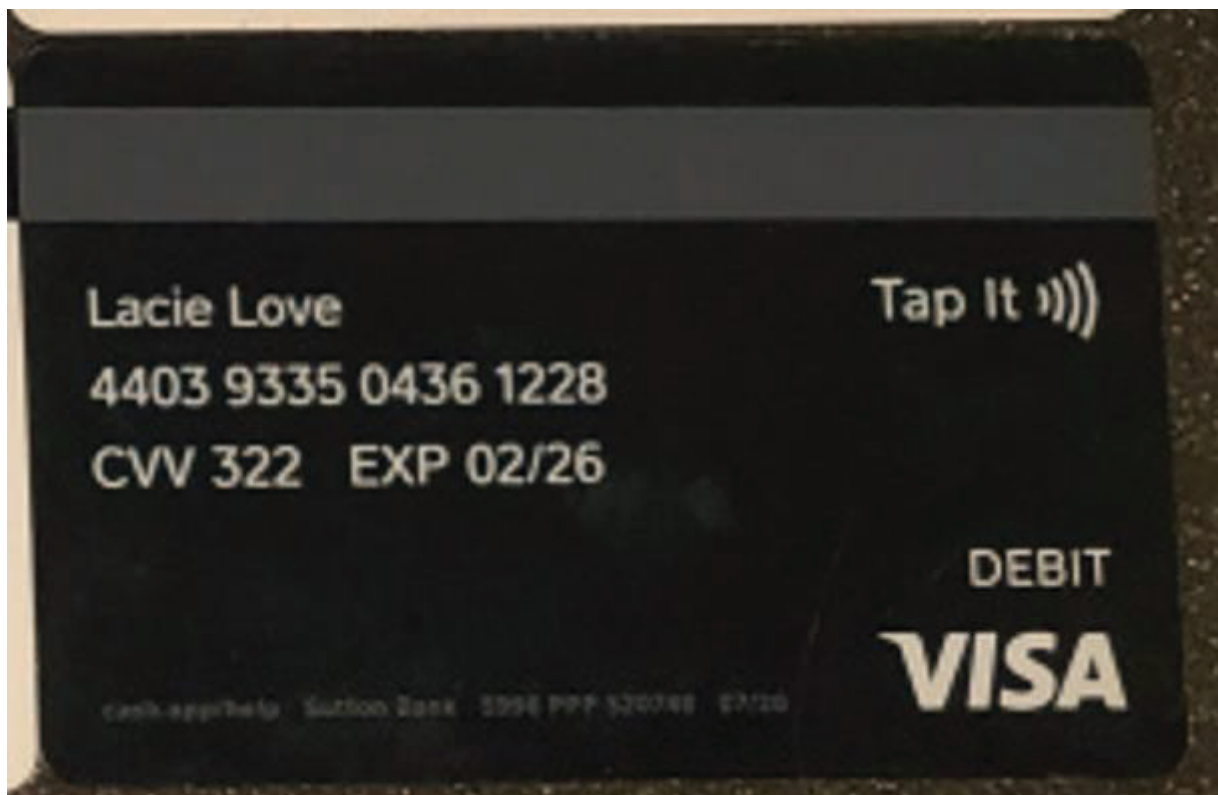




22. Law enforcement identified that the female in the picture shown in the above conversation was a 14-year-old minor female (henceforth named MFV-2). Law enforcement interviewed MFV-2, which stated they were not in control of the “laciexlove69” Snapchat account at the time of the conversation with SUBJECT BUYER in March 2022.
23. Moreover, the lawful search of the SUBJECT BUYER Phone revealed that sexually explicit videos discussed in the above pictured conversation between SUBJECT BUYER and “LaciexLove69 – Lacie” were sent by Snapchat username “Laciexlove69” to SUBJECT BUYER within the Snapchat application and within a secondary

communication application, Telegram. Law enforcement identified the individual in the explicit videos sent to SUBJECT BUYER, as MFV-2, and additionally a sixteen-year-old minor female (MFV-3), and a sixteen-year-old minor male (MMV-1). Law enforcement identified payments for the videos of MFV-2, MFV-3, and MMV-1 were made by SUBJECT BUYER to Cash App account “Kandie Kae - \$kandiexkae69”.

24. Lawfully obtained records revealed that on or about August 3, 2020, Cash App account “Kandie Kae - \$kandiexkae69” added the customer address of “604 Upland Creek Road Columbia, Missouri 65201” to the account profile. The same “604 Upland Creek Road Columbia, Missouri 65201” address was added to the customer account again on September 6, 2020, and November 20, 2020. Furthermore, lawfully obtained records revealed that “Kandie Kae - \$kandiexkae69” debit cards #4403932023271967, #4403932032810284, and #4403933504361228 were activated utilizing the same “604 Upland Creek Road Columbia, Missouri 65201” address. Records also revealed that, in the same time period described above, prior to the “Kandie Kae - \$kandiexkae69” identifiers, the account utilized the following identifiers, “Lacie Love - \$laciexlove69”.



25. In or about May 2022, law enforcement identified Ryan Edward Hine (“HINE”) as a resident of 604 Upland Creek Road Columbia, Missouri:



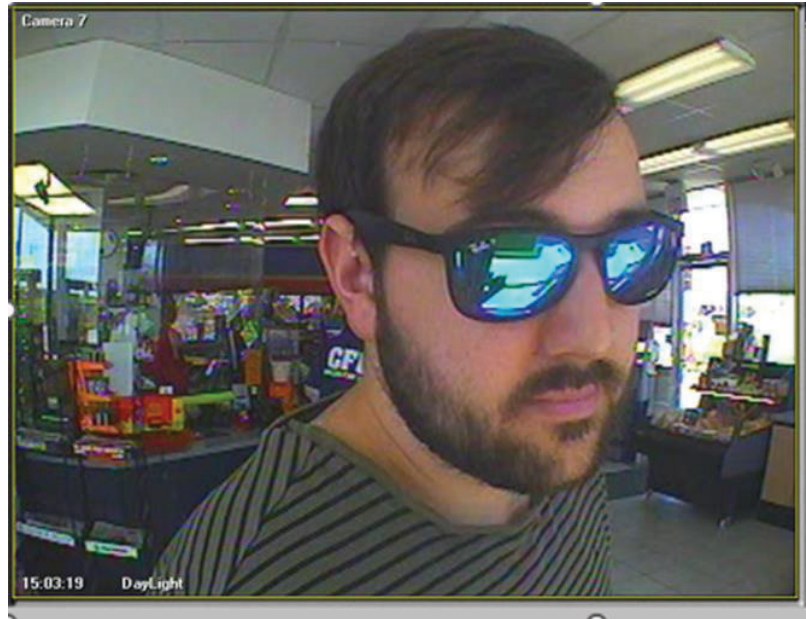
(Image of HINE driver’s license and Passport recovered from HINE September 2, 2022, during lawful search)

26. Law enforcement identified records produced by Cash App for “KANDIE KAE - \$kandiexkae69”, showing approximately twenty-three (23) ATM withdrawals, from in or around November 2020 through in or around May 2022, totaling approximately

\$8,918.00 USD, made at the same convenience store located at 900 Conley Road Columbia, MO. The Cash App debit cards for the KANDIE KAE account used for the 23 ATM withdrawals were sent to and activated at 604 Upland Creek Road Columbia, Missouri. The Cash App debit cards for the KANDIE KAE Cash App account were sent to the 604 Upland Creek Road, Columbia, Missouri address, to include the Cash App Visa Debit card #4403933504361228. Records from Cash App showed the card was created and activated on or about December 5, 2020 with the name “Lacie Love”.

27. On December 5, 2020, the above credit card, Visa Debit Card #4403933504361228 was activated, HINE changed the “\$cashtag” name from “\$Laciexlove69” to “\$kandiexkae69”.

28. In or around July 2022, law enforcement lawfully obtained security camera footage from the convenience store located at 900 Conley Road Columbia, Missouri for ATM withdrawals of May 1, 2022, for Cash App debit card #4403933504361228. Law enforcement observed an adult male matching the description of HINE conducting the ATM withdrawals on the same date and time identified by Cash App as seen in images below:



Law enforcement also observed that once the adult male from the images above both arrived and departed the parking lot of the convenience store in a grey colored four-door sedan:



29. In or around September 2, 2022, **HINE** was encountered by law enforcement during an inbound, international land border arrival into the United States from Toronto, Canada. Subsequent to HINE's arrival at the Ambassador Bridge Port of Entry in Detroit, Michigan, law enforcement conducted a lawful inspection and search of **HINE**, his vehicle, and all merchandise in his possession which were presented at the port of entry. Law enforcement recovered a wallet from HINE, and photographed the following images from **HINE's** wallet contents, to include Cash App debit card #4403933504361228 with inscription "Lacie Love":



30. Additionally, Visa Gift Card #4250975652022833 was identified during the border search of HINE on September 2, 2022. The same card was linked to PayPal Account “Lacie Love – laciexlove69@gmail.com” on or about May 7, 2020 per PayPal records. Analysis of the “Kandie Kae \$kandiexkae69” (previously \$laciexlove69) Cash App account identified that the “Lacie Love – laciexlove69@gmail.com” Paypal account made 4 transfers totaling \$1,473.88 USD from August 2, 2020 to August 16, 2020. This

is the same July 2020 through September 2020 timeframe that we identified text conversation between HINE and victim MV3 that HINE was in control of the \$laciexlove69 Cash App account.



31. HINE's vehicle, in which he made entry into the United States at the Ambassador Bridge Port of Entry in Detroit, Michigan, is pictured below:

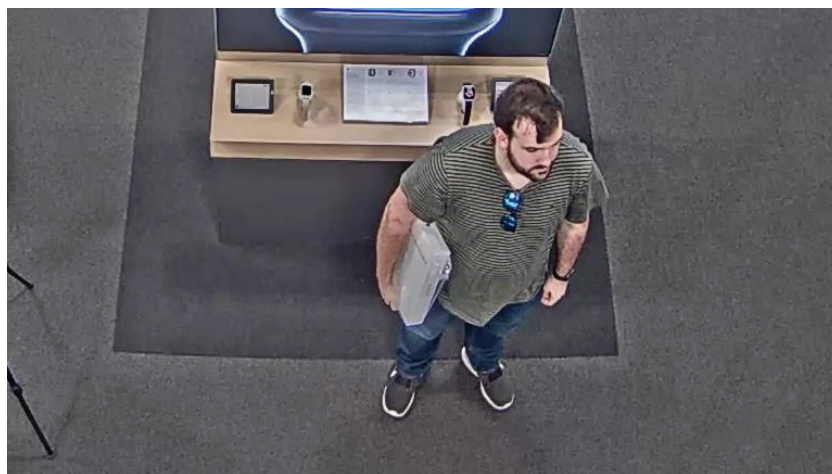


32. Additionally, law enforcement discovered multiple electronic devices in HINE's possession at the time of his arrival at the port of entry. HINE's electronic devices were subsequently seized on September 2, 2022. Law enforcement identified the following images recovered from HINE's iPhone seized September 2, 2022:



(Images recovered from HINE's cellular device which was seized September 2, 2022)

33. Law enforcement observed an adult male wearing a similar patterned shirt, with similar physical and facial features making ATM withdrawals at 900 Conley Road Columbia, Missouri on May 1, 2022, for Cash App debit card #4403933504361228.
34. In or around January 2023, law enforcement also recovered surveillance video from Best Buy Store #602 in Columbia, Missouri from a November 11, 2022, purchase made by HINE, who appears to be wearing the same shirt from the ATM video, utilizing his Best Buy rewards membership card account:



35. On the next day, November 12, 2022, HINE returned to the same Best Buy #602 store and purchased “TMO IPHONE 14 PRO MAX 128GB DEEP PURPLE, IMEI# 350387751322204, MDN/Mobile Phone Number: 3127317662”. Law enforcement identified through T-Mobile records that this iPhone is registered to an active account at 604 Upland Creek Road, Columbia, Missouri.

36. Law enforcement identified that in or around June 2022, HINE vacated his leased apartment in Chicago, Illinois. Additionally, in statements made to law enforcement in September 2022, October 2022, and January 2023, HINE identified that his current address is 604 Upland Creek Road, Columbia, Missouri.

37. A check with public database systems on or about January 8, 2023, revealed that an Edward Hine (Date of Birth XX,XX, 1961), a Lisa Hine (Date of Birth XX,XX, 1960), a Logan Hine (Date of Birth XX,XX, 2001), and a Ryan HINE (Date of Birth XX, XX, 1996), residing at the SUBJECT PREMISES.

38. On January 12, 2023, your affiant conducted surveillance of the SUBJECT PREMISES. A tan color Lexus with Missouri plates LF2 Y7K was observed at the SUBJECT PREMISES. A further check on government systems revealed this vehicle belonging to a Edward and Lisa Hine. Your affiant also observed a dark color sedan with temporary tags parked in front of the residence.

39. On or about January 13, 2023, an HSI Special Agent contacted HINE and confirmed HINE residing at the SUBJECT PREMISES.

40. On January 5, 2023, your affiant used his government-issued iPhone in an effort to gain additional information regarding any potential wireless networks at the SUBJECT

PREMISES. Positioned approximately ten (15) yards from the SUBJECT PREMISES, your affiant noted that there were multiple wireless networks in the area, but all of them were secured. Accordingly, to use any of them to access the Internet, a user would likely have to know the encryption key or password for that particular network. Based on the signal strength of the wireless networks, as well as my training and experience and information relayed to me by agents, your affiant believes that the wireless router at the SUBJECT PREMISES is likely generating a secured wireless network. As explained above, I know, from my training and experience and information relayed to me by agents, that wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime.

41. It is your affiants believe that HINE is in control of the Cash App account “Kandie Kae - \$kandiexkae69”, formally known as “Lacie Love - \$laciexlove69”. It is also your affiants believe that HINE would be in possession of child exploitation material, that could be found on his devices.

**CHARACTERISTICS OF INDIVIDUALS WHO RECEIVE AND COLLECT IMAGES
OF CHILD PORNOGRAPHY**

42. Based upon my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

- a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature

describing such activity.

- b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Collectors of child pornography almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, to enable the collector to view the collection, which is valued highly.
- e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child

pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

- f. Collectors of child pornography prefer to have continuous access to their collection of child pornography. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

43. Based upon the conduct of individuals involved in the collection of child pornography set forth above, namely, that they tend to maintain their collections at a secure, private location for long periods of time, there is probable cause to believe that evidence of the offenses of receiving and possessing child pornography is currently located at the premises described previously herein, known as, and the computers and computer media located therein.

SEIZURE OF EQUIPMENT AND DATA

44. Based upon my knowledge, training and experience, I know that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, to ensure accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that some computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, be seized and subsequently processed by a qualified computer specialist in a laboratory setting. This is true because of the following:

- a. The volume of evidence. Computer storage devices (such as hard disks, diskettes, tapes, laser disks, etc.) can store the equivalent of thousands of pages of information. Additionally, a user may seek to conceal criminal evidence by storing it in random order with deceptive file names. Searching authorities are thus required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process may take weeks or months, depending on the volume of data stored and it would be impractical to attempt this kind of data analysis on-site.
- b. Technical requirements. Analyzing computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know prior to the search which expert possesses sufficient specialized skills to best analyze the system and its data. No matter which system is used, however, data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even “hidden”, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system as a “booby trap”), a controlled environment is essential to its complete and accurate analysis.

45. Due to the volume of the data at issue and the technical requirements set forth above, it may be necessary that the above-referenced equipment, software, data, and related instructions be seized and subsequently processed by a qualified computer specialist in a laboratory setting. Under appropriate circumstances, some types of computer equipment can be more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal from the premises. One factor used in determining whether to analyze a computer on-site or to remove it from the premises is whether the computer constitutes an instrumentality of an offense and is thus subject to immediate seizure as such-- or whether it serves as a mere repository for evidence of a criminal offense. Another determining factor is whether, as a repository for evidence, a particular device can be more readily, quickly, and thus less intrusively analyzed off site, with due consideration given to preserving the integrity of the evidence. This, in turn, is often dependent upon the amount of data and number of discrete files or file areas that must be analyzed, and this is frequently dependent upon the particular type of computer hardware involved. As a result, it is ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized.

46. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - -

that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

47. Based upon my knowledge, training, and experience, and the experience of other law enforcement personnel with whom I have spoken, I am aware that searches and seizures of evidence from computers taken from the subject premises commonly require agents to seize most or all of a computer system's input/output peripheral devices, in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. Therefore, in those instances where computers are removed from the subject premises, and in order to fully retrieve data from a computer system, investigators must seize all magnetic storage devices as well as the central processing units (CPU) and applicable keyboards and monitors which are an integral part of the processing unit. If, after inspecting the input/output devices, system software, and pertinent computer-related documentation it becomes apparent that these items are no longer necessary to retrieve and preserve the data evidence, such materials and/or equipment will be returned within a reasonable time.

48. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

COMPUTER EXAMINATION METHODOLOGY TO BE EMPLOYED

49. The examination procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other examination procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BIOMETRIC ACCESS

50. Many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

51. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called

“Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. The fingerprints authorized to access the particular device are a part of the security settings of the device and will allow access to the device in lieu of entering a numerical passcode or longer alpha-numerical password, whichever the device is configured by the user to require. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

52. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. Apple’s facial recognition feature is referred to as Face ID and it allows a user to unlock the iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of the user’s face. Face ID confirms attention by detecting the direction of the user’s gaze, then uses neural networks for matching and anti-spoofing so the user can unlock the phone with a glance. Face ID automatically adapts to changes in the user’s appearance, and carefully safeguards the privacy and security of the user’s biometric data. Similarly, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices

produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

53. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

54. Beginning with the release of Apple's iOS 8 operating system in September 2014, Apple no longer has a key to decrypt these devices. Thus, even with a properly authorized search warrant to gain access to the content of an iOS device, there is no feasible way for the government to search the device.

55. Users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

56. As discussed in this Affidavit, there is reason to believe that one or more digital electronic devices, (Device(s)), will be found during the search. The passcode or password that

would unlock any Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

57. Biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Further, Touch ID will not allow access if the device has been turned off or restarted, if the device has received a remote lock command, or if five attempts to match a fingerprint have been unsuccessful. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

58. A person who is in possession of a Device or has the Device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via biometric data, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty

who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device.

CONCLUSION

59. Based on the above information, there is probable cause to believe that the SUBJECT OFFENSES have been violated, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES described in Attachment A, and any computers, computer media, or wireless telephones therein, and more fully described herein. Your Affiant requests authority to seize such material, specifically, that the Court issue a search warrant for these premises and all computers, computer hardware and media, and wireless telephones therein.

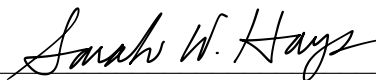
I state under the penalty of perjury that the foregoing is true and correct.

THOMAS H
PUTTING

Digitally signed by
THOMAS H PUTTING
Date: 2023.02.03
12:02:42 -06'00'

THOMAS PUTTING
Special Agent
Homeland Security Investigations

Attested to in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone or other reliable electronic means on February 3rd, 2023.



Sarah W. Hays
UNITED STATES MAGISTRATE JUDGE